Aplikasi Enkripsi dan Dekripsi *Short Message Service* di Android Menggunakan Metode Blowfish

Wildatunnisa Fahriah[1*)], Tulus Febrianto[2]
[1]Program Studi Sistem Informasi, STTI NIIT I-Tech
[2] Program Studi Sistem Informasi, STTI NIIT I-Tech
email: [1]wilda184@gmail.com, [2]titu.tf@gmail.com

Abstrak **Layanan pesan singkat (SMS) adalah teknologi komunikasi yang sangat populer. Dengan menggunakan SMS seseorang dapat bertukar pesan dengan orang lain. Namun, dengan masalah penyadapan sms, seseorang tidak lagi memiliki hak privasi. Program dibuat pada aplikasi berbasis ponsel yang akan mengubah pesan SMS android menjadi kode sehingga informasi dari SMS tidak diketahui oleh orang lain. Saat mengirim SMS, tidak diketahui oleh orang lain. Saat mengirim SMS, aplikasi ini akan mengenkripsi pesan menjadi bentuk dengan kode kunci yang dimasukkan oleh pengirim. Dan ketika penerimaan SMS, aplikasi ini akan menggambarkan kode pesan ke dalam bentuk pesan asli menggunakan kunci yang sama dengan pengirim. Aplikasi ini dibuat dalam aplikasi berbasis android untuk mengirim pesan penting kepada orang lain tanpa takut diperhatikan oleh orang lain. Metode yang digunakan dalam aplikasi untuk mengenkripsi dan mendepkripsi pesan yaitu metode Algoritma Block Cipher atau yang biasa disebut Blowfish dan implementasinya menggunakan bahasa pemrograman java dengan platfrom mobile android.**
Kata Kunci **– SMS, Enkripsi, Depkripsi, Block Cipher, Blowfish, Java.**

Abstract – Short Message Service (SMS) is a communication technology that is very popular. By using SMS someone can exchange messages with others. However, with the wiretapping issue sms, a person no longer has the right to privacy. So the program was made on a mobile phone-based application that will change the android SMS messages into codes so that information from SMS in not known by others. When sending SMS, this application will encrypt the message into shape with a key codes entered by the sender. And when the acceptance of SMS, this application will describe the codes message into form of the original message using the same key with the sender. This application was made in the android based application to send an important message to others without fear of being noticed by others. The method used in the application to encrypt and decrypt the messages are methods Block Cipher Algorithm or also called blowfish method and its implementation using the java programming language with the android mobile platform.
Keywords – SMS, Encrypt, Decrypt, Blok Cipher, blowfish, Java.

I. PENDAHULUAN

Kebutuhan masyarakat untuk berkomunikasi secara tidak langsung membuat terciptanya metode pengiriman pesan pada zaman tradisional yaitu dengan surat. Tetapi, dengan surat, pengiriman pesan dapat sampai dalam waktu yang lama. Perkembangan teknologi membuat lahirnya sebuah alat yang merupakan cikal bakal terbentuknya *Short Messaging Service* (SMS) yaitu pager. Namun, dengan kebutuhan masyarakat akan pengiriman pesan dengan cepat, akurat dan aman membuat para ahli teknologi menciptakan sebuah alat yaitu ponsel. Ponsel atau *mobile* pertama kali diciptakan sudah dilengkapi dengan fitur SMS. Teknologi SMS dikembangkan pertama kali oleh Friedhelm Hillebrand, Bernard Ghillebaert, dan Oculy Silaban. Kemudian muncullah organisasi-organisasi yang menciptakan standar teknologi SMS sehingga membuat teknologi SMS bisa digunakan di seluruh dunia. Dikembangkannya standarisasi SMS dimulai tahun 1985 oleh upaya kerja sama antara Perancis dan Jerman. Saat sebuah pesan atau data menjadi penting dan bersifat privasi maka perlu diadakan perlindungan terhadap data tersebut. Oleh karena itu, para pakar menciptakan sebuah metode algoritma untuk mengamankan data. Metode ini disebut metode enkripsi dan deskripsi. Metode pengamanan data di luar negeri memang sudah dilakukan sejak dahulu. Contohnya di Inggris sebuah perusahaan operator telepon selular staellium UK mengeluarkan layanan bernama "*stealth text*" yang dapat digunakan untuk mengirim pesan secara aman karena pesan akan terhapus jika pesan telah terbaca. Masalah umum tentang keamanan data melalui SMS yaitu masalah pesan yang dikirim oleh seseorang dapat disadap oleh orang ketiga sehingga pesan yang disampaikan tidak sama dengan pesan yang dikirim. Tujuan yang dicapai adalah agar dapat menghasilkan aplikasi enkripsi dan deskripsi SMS berbasis Android yang digunakan untuk mengirim dan menerima pesan teks dengan mengamankan atau menyembunyikan pesan asli, sehingga pengirim tidak perlu takut pesannya akan disadap dan diketahui orang lain. Terdapat beberapa cara dalam menerapkan keamanan pada pesan yaitu steganografi dan enkripsi. Pada penelitian ini akan menggunakan enkripsi sebagai cara dalam pengamanan pesan SMS.

II. TINJAUAN PUSTAKA

A. *Kriptografi*

Crypto berarti secret (rahasia) dan *graphy* berarti *writing* (tulisan). Jadi, kriptografi berarti *secret writing* (tulisan rahasia). Menurut Munir (2006, h.2), definisi kriptografi ada dua, yaitu:

1) Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan.

 ISSN: 2614-8404

2) Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi.

B. Algoritma Blowfish

Blowfish merupakan blok cipher 64-bit dengan panjang kunci *variabel*. Algoritma ini terdiri dari dua bagian: *key expansion* dan enkripsi data. *Key expansion* merubah kunci yang dapat mencapai 448 bit menjadi beberapa *array* subkunci (*subkey*) dengan total 4168 *byte*. Enkripsi data terdiri dari iterasi fungsi sederhana sebanyak 16 kali. Setiap putaran terdiri dari permutasi kunci-dependent dan substitusi kunci dan data-dependent. Semua operasi adalah penambahan dan XOR pada *variable* 32-bit. Tambahan operasi lainnya hanyalah empat penelusuran tabel (*table lookup*) *array* berindeks untuk setiap putaran. *Blowfish* menggunakan subkunci yang besar. Kunci ini harus dihitung sebelum enkripsi atau dekripsi data. *Array* P terdiri dari delapan belas 32-bit subkunci:

P1,P2, . . . ,P18

Empat 32-bit S-box masing-masing mempunyai 256 entri:

S1,0, S1,1, . . . , S1,255
S2,0, S2,1, . . . , S2,255
S3,0, S3,1, . . . , S3,255
S4,0, S4,1, . . . , S4,255

Blowfish merupakan algoritma yang menerapkan jaringan Feistel (*Feistel network*) yang terdiri dari 16 putaran. Input merupakan elemen 64 bit, X. Untuk mengenkrip:

1) Bagi X menjadi dua 32-bit: XL, XR
2) untuk i = 1 sampai 16
   a) XL = XL xor Pi
   b) XR = F(XL) xor XR
   c) Tukar XL dan XR
   d) Tukar XL dan XR (batalkan penukaran terakhir)
   e) XR = XR xor P17
   f) XL = XL xor P18
3) Kombinasikan kembali XL dan XR

Fungsi F adalah sebagai berikut:

1) Bagi XL, menjadi empat bagian 8-bit: a, b, c dan d
2) F(XL) = ((S1,a + S2,b mod 232) xor S3,c) + S4, c mod 232

Dekripsi sama persis dengan enkripsi, kecuali P1, P2, ..., P18 digunakan pada urutan yang terbalik. Subkunci dihitung menggunakan algoritma *Blowfish*, metodanya adalah sebagai berikut:

1) Pertama-tama inisialisasi P-array dan kemudian empat S-box secara berurutan dengan *string* yang tetap. *String* ini terdiri digit hexadesimal dari pi.
2) XOR P1 dengan 32 bit pertama kunci, XOR P2 dengan 32 bit kedua dari kunci dan seterusnya untuk setiap bit dari kunci (sampai P18). Ulangi terhadap bit kunci sampai seluruh P-*array* di XOR dengan bit kunci.
3) Enkrip semua string nol dengan algoritma *Blowfish* dengan menggunakan subkunci seperti dijelaskan pada langkah (1) dan (2).
4) Ganti P1 dan P2 dengan keluaran dari langkah (3)
5) Enkrip keluaran dari langkah (3) dengan algoritma *Blowfish* dengan subkunci yang sudah dimodifikasi.
6) Ganti P3 dan P4 dengan keluaran dari langkah (5).
7) Lanjutkan proses tersebut, ganti seluruh elemen dari P-*array*, dan kemudian seluruh keempat S-box berurutan, dengan keluaran yang berubah secara kontinyu dari algoritma *Blowfish*.

Total diperlukan 521 iterasi untuk menghasilkan semua subkunci yang dibutuhkan. Aplikasi kemudian dapat menyimpan subkunci ini dan tidak dibutuhkan langkah-langkah proses penurunan ini berulang kali, kecuali kunci yang digunakan berubah.

C. Tinjauan Penelitian Terkait

Penelitian yang di lakukan oleh Hendrayanto, Rudy dan A. Ramadona Nilawati dengan judul Aplikasi Enkripsi dan Deskripsi SMS pada Ponsel Berbasis Android dengan Algoritma DES. Dalam tulisan ini peneliti menggunakan algoritma DES, dan program aplikasi SMSCrypt menggunakan struktur navigasi jenis campuran yang menggabungkan navigasi struktur hirarki dengan struktur navigasi linier. Struktur navigasi hirarki terdaftar di Main Menu memiliki percabangan Tulis Pesan, *Inbox*. Sedangkan struktur navigasi linier Tulis pesan tercetak pada halaman dan inbox, di mana aktivitas di halaman dilakukan secara berurutan . SMSCrypt struktur navigasi Program, program aplikasi SMSCrypt telah berhasil dibuat dan diuji di Android emulator . Hasil dari program percontohan setelah aplikasi dijalankan menggunakan *Eclipse Indigo*.

Penelitian yang di lakukan oleh Wijaya, Aris Kusuma, Martinus dan Abdul Rahman dengan judul Rancang Bangun Aplikasi Enkripsi dan Dekripsi Berbasis Android dengan Menggunakan Algoritma Hybrid DES dan Elgamal. Dalam tulisan ini peneliti telah membuat aplikasi enkripsi dan dekripsi pesan pada ponsel berbasis Android dengan menggunakan algoritma hybrid DES dan ElGamal dapat menjaga kerahasiaan pesan, mudah digunakan, bekerja dalam fungsi sesuai, memenuhi kebutuhan standar, *user friendly* dengan aplikasi antarmuka yang cukup menarik.

Penelitian yang di lakukan oleh Irwan dengan judul Perancangan Aplikasi SMS (*Short Message Service*) dengan Enkripsi Teks Menggunakan Algoritma Block Cipher AES (*Advanced Encryption Standart*) Berbasis *Mobile* Pada *Platform Android*. Dalam hal ini peneliti jurnal membuat aplikasi android yang dibuat bernama AES SMS Plus. AES SMS Plus merupakan aplikasi SMS dengan enkripsi teks menggunakan algoritma AES di enkripsi dan dekripsi proses. Secara garis besar, sebuah SMS aplikasi alur kerja dengan algoritma enkripsi teks menggunakan *block cipher* AES. Pengguna dapat melakukan aktivitas menulis pesan dan mengenkripsi pesan sebelum dikirim dengan memasukkan kunci tertentu, atau segera dapat mengirim pesan tanpa enkripsi. Jika pengguna menggunakan fitur enkripsi untuk mengirim pesan, maka pengguna dapat menyimpan Kunci kotak kunci setelah itu dikirim. Pengguna dapat membaca pesan langsung atau

ISSN: 2614-8404

mendekripsi pesan dengan memasukkan kunci secara langsung atau dengan mengakses kotak kunci. Pengguna dapat mengakses kotak kunci untuk melihat daftar kunci yang disimpan atau mendaftar kunci baru. Pengguna dapat mengakses bantuan yang berisi tentang deskipsi dan pedoman fitur penggunaan aplikasi.

III. METODE PENELITIAN

Metodologi yang digunakan untuk perancangan Aplikasi Pengenkripsian dan Pendeskripsian SMS pada Android menggunakan metode Algoritma *Block Cipher* atau *Blowfish Method* adalah *Prototype*. Penulis menggunakan metode *Prototype* yang dibagi dalam 4 fase sebagai berikut :

A. Analisis Kebutuhan Sistem

Pada tahap ini penulis melakukan analisis kebutuhan sistem yang meliputi ruang lingkup, kebutuhan *user*, pemecahan masalah, logika prosedural. Analisis kebutuhan *user* dibagi dua, yaitu kebutuhan fungsional dan non fungsional.

B. Desain Sistem

Analisis sistem (*system analysis*) mendeskripsikan apa yang harus dilakukan sistem untuk memenuhi kebutuhan informasi pemakai. Desain sistem (*system design*) menentukan bagaimana sistem akan memenuhi tujuan tersebut. Desain sistem terdiri dari aktivitas desain yang menghasilkan spesifikasi fungsional. Desain sistem dapat dipandang sebagai desain *interface*, data dan proses dengan tujuan menghasilkan spesifikasi yang sesuai dengan produk dan metode *interface* pemakai, struktur database serta pemrosesan dan prosedur pengendalian (Ioanna et al., 2007). Tahap ini merancang tampilan (*interface*), *package* diagram, dan sebagainya dijelaskan pada bab 3.

C. Pengujian Sistem

Pada tahap ini penulis melakukan pengujian, memverifikasi interaksi aplikasi yang telah dibuat dan mengimplementasikan semua *requirements* dengan tujuan menghasilkan tujuan yang telah dirumuskan pada tahap *Business Modelling* atau *Business Engineering*. Pengujian dilakukan sebelum penyerahan aplikasi kepada *user*.

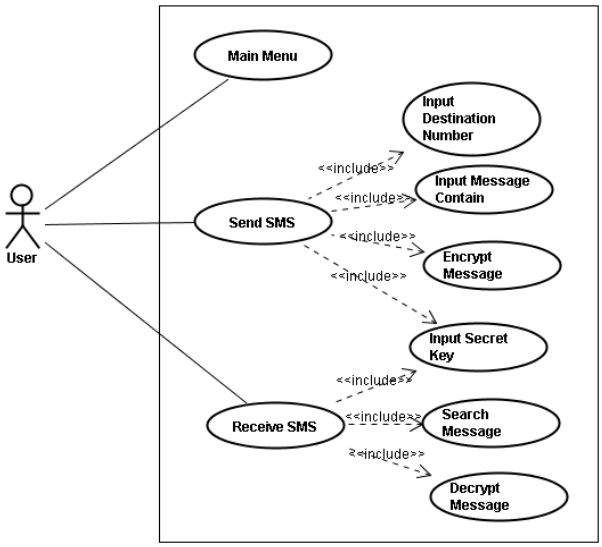
D. Implementasi

Pada tahap ini penulis membuat perangkat lunak berdasarkan arsitektur yang telah dibuat pada tahap *analysis and design* dalam bentuk coding, dan memiliki perilaku seperti yang telah dimodelkan pada tahap *requirements* dengan mengimplementasikan *usecase*.

IV. HASIL DAN PEMBAHASAN

A. Use case Diagram

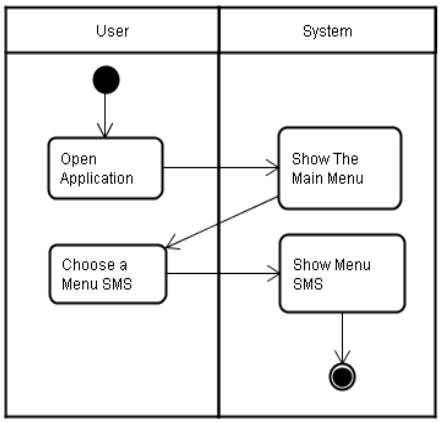
Berikut ini adalah diagram usecase pada Aplikasi Enkripsi dan Deskripsi SMS di Android Menggunakan Metode *Blowfish*.



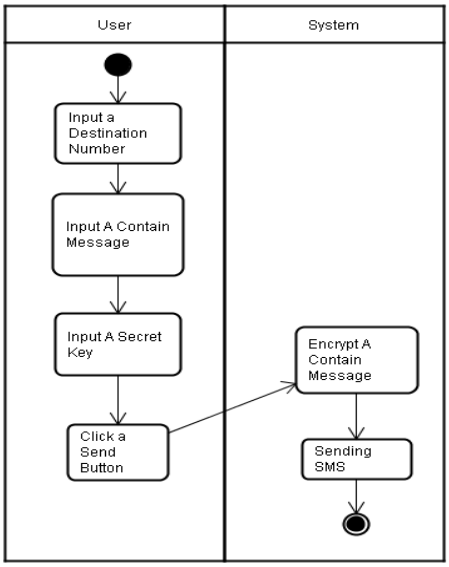
Gambar 1.*Use case* Diagram

B. Activity Diagram

Berikut ini adalah diagram aktivitas pada Aplikasi Enkripsi dan Deskripsi SMS di Android Menggunakan Metode *Blowfish*.

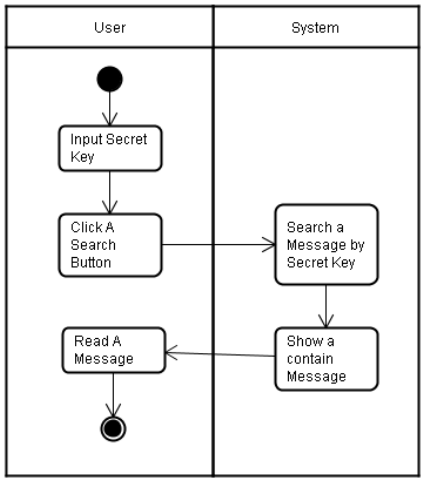


Gambar 2.*Activity* Diagram



Gambar 3.*Activity* Diagram

 ISSN: 2614-8404

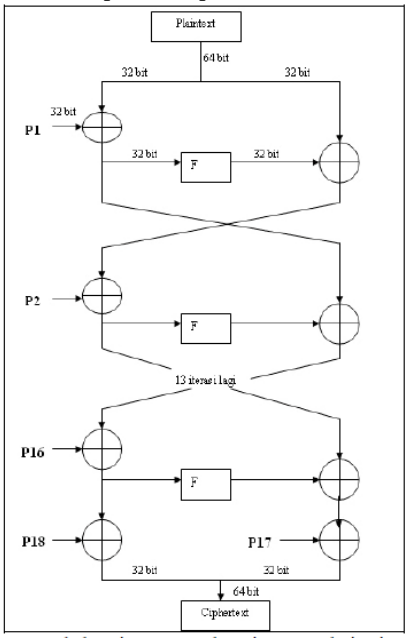


Gambar 4.*Activity* Diagram

C. Proses Sistem

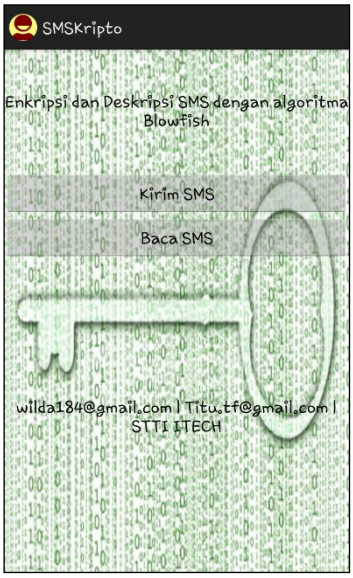
Berikut adalah cara enkripsi metode *blowfish*. Terdiri dari fungsi iterasi sederhana (*Feistel Network*) 16 kali putaran (iterasi), adalah 64-bit X. elemen data masukan Setiap putaran terdiri dari permutasi kunci dependent dan substitusi kunci dan data tergantung. Semua operasi adalah penambahan dan XOR pada variabel 32-bit. Sebuah operasi tambahan hanya empat meja pencarian diindeks *array* untuk setiap putaran. Langkah-langkahnya adalah sebagai berikut. Untuk X menjadi dua bagian, yang masing-masing terdiri dari 32 - bit : XL, XR . Lakukan langkah-langkah berikut.

1) Untuk i = 1 sampai 16 :
   XL = XLØ Pi
   XR = F(XL) Ø XR
   TukarXL dan XR
2) Setelah iterasi ke-16, tukarlah XL dan XR lagi untuk membatalkan pertukaran lalu.
3) Kemudian lakukan
   XR = XRØ P17
   XL = XLØ P18
4) Akhirnya, menggabungkan kembali XL dan XR untuk mendapatkan *ciphertext*.



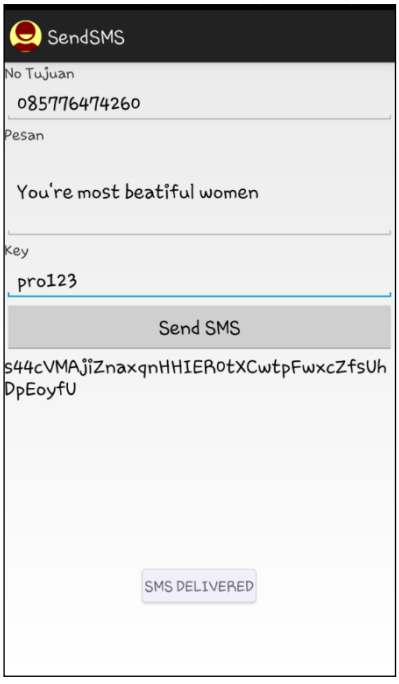
Gambar 5.Proses Enkripsi *Blowfish*

Berikut ini adalah implementasi dalam bentuk antarmuka aplikasi. Ini adalah tampilan utama dari aplikasi. Menu utama ini tersedia dalam dua pilihan, kirim sms dan membaca sms. Jika mengklik sms, aplikasi akan membuka halaman untuk mengirim sms, dan jika Anda mengklik menu membaca sms, aplikasi akan membuka halaman membaca sms.



Gambar 6.Antarmuka Menu Utama Aplikasi

Berikut adalah halaman menu kirim SMS. Saat mengirim pesan, pengirim harus memasukkan jumlah penerima tujuan, pesan teks, dan kunci yang digunakan untuk membuka atau menggambarkan SMS dienkripsi.

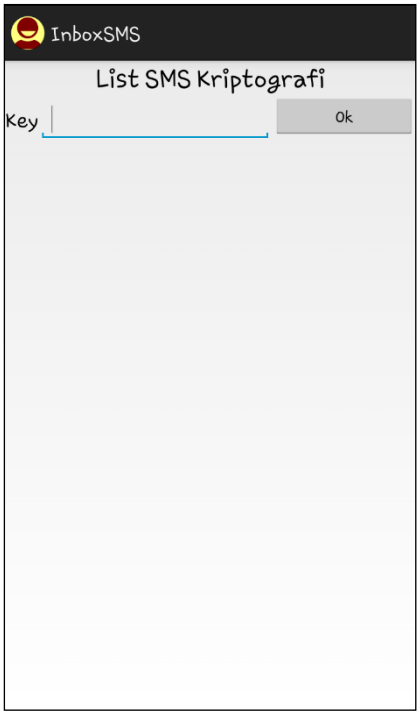


Gambar 7.Pengiriman SMS

Setelah pengirim mengirimkan sms dengan menekan tombol kirim SMS, maka akan muncul hasil enkripsi sms yang dikirim. Hasil enkripsi yang akan masuk ke penerima telepon selular dan menunjukkan pemberitahuan bahwa SMS telah dikirim.

 ISSN: 2614-8404

Berikut adalah screenshot dari menu Baca SMS. Dalam menu ini penerima harus memasukkan kunci yang diberikan oleh pengirim, sebagai cara untuk menggambarkan teks yang dikirim oleh pengirim. Kunci ini bersifat rahasia.



Gambar 7.Pengiriman SMS

V. PENUTUP

Keamanan teks menjadi masalah besar terutama dalam hal *mobile banking*, pesan yang membawa informasi rahasia, seperti M-*Commerce* dll sangat sulit untuk memecahkan karena kritografi yang dipakai menggunakan metode *Blowfish*, yang terdiri dari 16 putaran, dengan memasukkan 64 elemen bit. Dalam jurnal ini, metode *blowfish* untuk enkripsi dan dekripsi aplikasi disajikan untuk lingkungan berbasis Android. Sistem yang disajikan mampu untuk *encode* dan *decode* teks SMS untuk ponsel pintar. Hasil yang diperoleh menunjukkan kinerja yang efektif.

DAFTAR PUSTAKA

[1] S. M. Metev & V. P. Veiko, *Laser Assisted Microtechnology*, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.
[2] J. Breckling, Ed., *The Analysis of Directional Time Series: Applications to Wind Speed and Direction*, seri Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.
[3] S. Zhang, C. Zhu, J. K. O. Sin, &P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," *IEEE Electron Device Lett.*, vol. 20, pp. 569–571, Nov. 1999.
[4] M. Wegmuller, J. P. von der Weid, P. Oberson, & N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," *Prosiding ECOC'00*, 2000, paper 11.3.4, p. 109.
[5] R. E. Sorace, V. S. Reinhardt, &S. A. Vaughn, "High-speed digital-to-RF converter," U.S. Patent 5 668 842, Sept. 16, 1997.
[6] (2002) The IEEE website. [Online].Tersedia: http://www.ieee.org/
[7] M. Shell. (2002) IEEEtran homepage on CTAN. [Online]. Tersedia: http://www.ctan.org/tex-archive/macros/latex/contrib/supported/IEEEtran/
[8] *FLEXChip Signal Processor (MC68175/D)*, Motorola, 1996.
[9] "PDCA12-70 data sheet," Opto Speed SA, Mezzovico, Switzerland.
[10] A. Karnik, "Performance of TCP congestion control with rate feedback: TCP/ABR and rate adaptive TCP/IP," M. Eng. thesis, Indian Institute of Science, Bangalore, India, Jan. 1999.
[11] J. Padhye, V. Firoiu, &D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control," Univ. of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999.
[12] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Std. 802.11, 1997.
[13] Yaddarabullah, AZ Nazori. 2016. Pemanfaatan Kompresi Huffman Untuk Optimasi Ukuran Gambar Pada Sistem Steganography Menggunakan Metode Least Significant Bit (LSB). Telematika MKOM, 7(1), pp 29-38